DNA Center for SWIM의 HTTPS 오류 트러블슈팅

목차

소개

이 문서에서는 Cisco IOS® XE 플랫폼의 Cisco DNA Center를 위한 SWIM 프로세스에서 HTTPS 프로토콜의 문제를 해결하기 위한 절차를 설명합니다.

사전 요구 사항

요구 사항

GUI에서 ADMIN ROLE(관리자 역할) 권한과 스위치 CLI를 사용하여 Cisco DNA Center에 액세스해야 합니다.

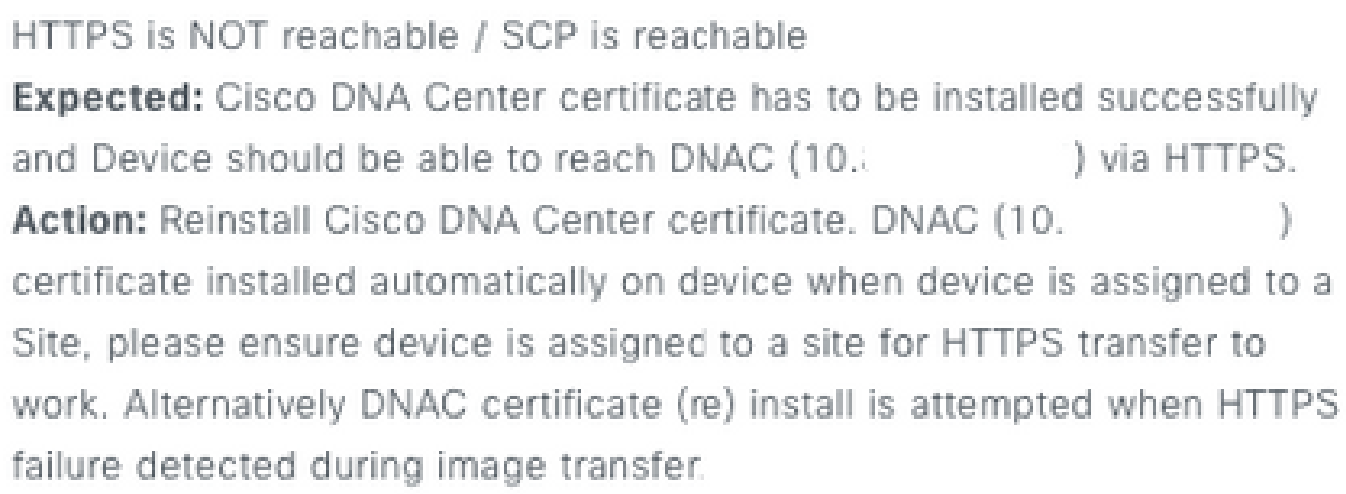
사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

이미지 업데이트 준비 상태 점검 후 Cisco DNA Center/SWIM(Software Image Management)에 표시되는 일반적인 오류가 있습니다.

"HTTPS에 연결할 수 없음/SCP에 연결할 수 있음"



이 오류는 HTTPS 프로토콜에 연결할 수 없음을 나타냅니다. 그러나 Cisco DNA Center에서 SCP 프로토콜을 사용하여 Cisco IOS® XE 이미지를 네트워크 디바이스로 전송합니다.

SCP를 사용하는 경우 단점 중 하나는 이미지를 배포하는 데 걸리는 시간입니다. HTTPS가 SCP보다 빠릅니다.

확인

Cisco DNA Center 인벤토리의 네트워크 디바이스 상태

Provision(프로비저닝) > Inventory(인벤토리) > Change Focus to Inventory(포커스를 인벤토리로 변경)로 이동합니다

업그레이드할 네트워크 장치의 연결성 및 관리성을 확인합니다. 디바이스의 상태는 Reachable and Managed여야 합니다.

네트워크 장치의 연결 및 관리 편의성에 다른 상태가 있는 경우 다음 단계로 이동하기 전에 문제를 해결하십시오.

네트워크 장치에 설치된 DNAC-CA 인증서

네트워크 디바이스로 이동하여 다음 명령을 실행합니다.

```
show running-config | sec crypto pki
```

DNAC-CA 신뢰 지점 및 DNAC-CA 체인을 확인해야 합니다. DNAC-CA 신뢰 지점, 체인 또는 둘 다가 표시되지 않는 경우 DNAC-CA 인증서를 푸시하려면 텔레메트리 설정을 업데이트해야 합니다.

디바이스 제어 기능이 비활성화되어 있으면 다음 단계를 수행하여 DNAC-CA 인증서를 수동으로 설치합니다.

- 웹 브라우저에서 https://<dnac_ipaddress>/ca/peman을 입력하고 .pem 파일을 다운로드합니다.
- .pem 파일을 로컬 컴퓨터에 저장합니다.
- 텍스트 편집기 응용 프로그램으로 .pem 파일 열기
- 네트워크 디바이스 CLI 열기
- 명령을 사용하여 이전 DNA-CA 인증서를 확인합니다. show run | in crypto pki trustpoint DNAC-CA

    - 이전 DNA-CA 인증서가 있는 경우 config 모드에서 명령을 사용하여 DNAC-CA 인증서 no crypto pki trustpoint DNAC-CA 를 제거합니다

    - DNAC-CA 인증서를 설치하려면 컨피그레이션 모드에서 명령을 실행합니다.

```
crypto pki trustpoint DNAC-CA
enrollment mode ra
enrollment terminal
usage ssl-client
revocation-check none
exit
crypto pki authenticate DNAC-CA
```

    - .pem 텍스트 파일 붙여넣기

    - 프롬프트가 표시되면 yes를 입력합니다

    - 설정 저장

문제 해결

포트 443을 통해 네트워크 디바이스에서 네트워크 디바이스의 Cisco DNA Center로 통신

네트워크 장치에서 HTTPS 파일 전송 테스트 실행

```
copy https://<DNAC_IP>/core/img/cisco-bridge.png flash:
```

이 테스트에서는 Cisco DNA Center에서 스위치로 PNG 파일을 전송합니다.

이 출력은 파일 전송이 성공했음을 나타냅니다.

```
MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
```

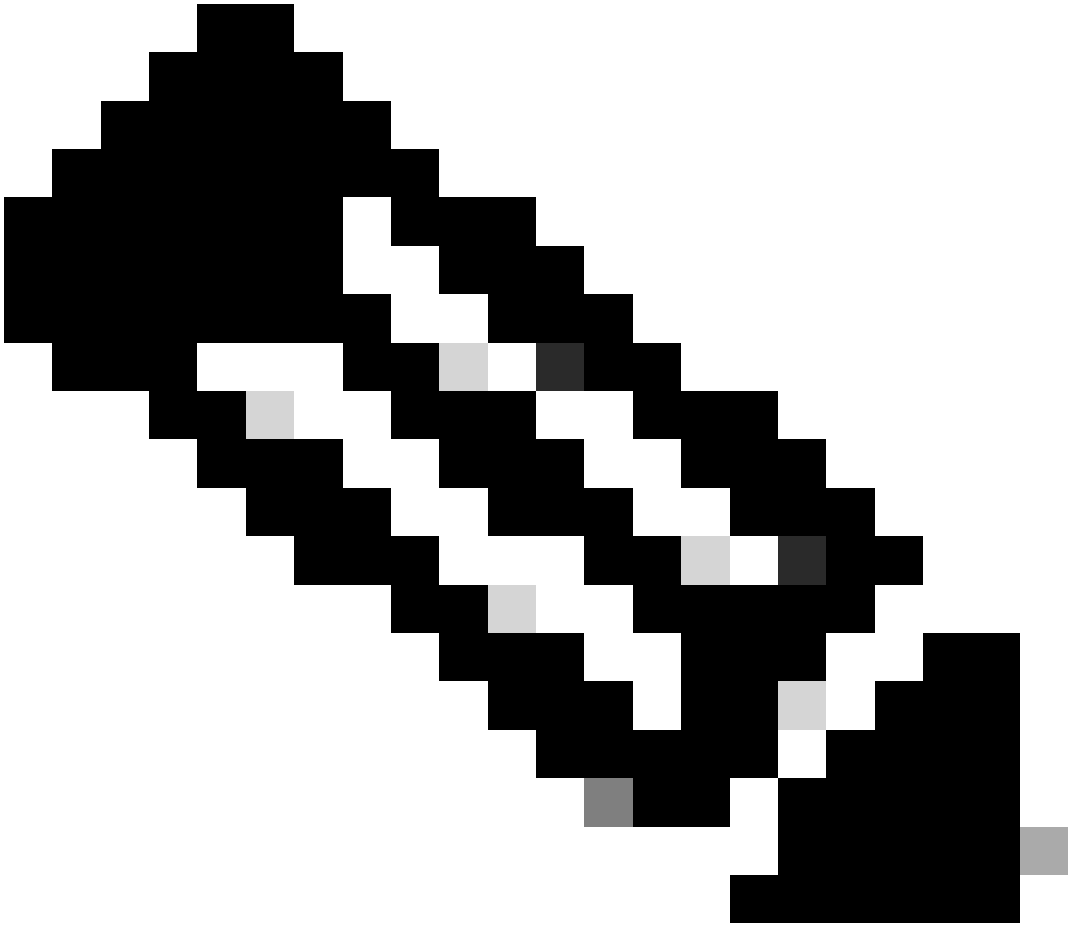
```
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
Loading https://10.x.x.x/core/img/cisco-bridge.png
4058 bytes copied in 0.119 secs (34101 bytes/sec)
MXC.TAC.M.03-1001X-01#
```

다음 출력을 가져오면 파일 전송에 실패했습니다.

```
MXC.TAC.M.03-1001X-01#$//10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
%Error opening https://10.x.x.x/core/img/cisco-bridge.png (I/O error)
MXC.TAC.M.03-1001X-01#
```

다음 작업을 수행합니다.

- 방화벽이 포트 443, 80, 22를 차단하고 있는지 확인합니다.
- 네트워크 디바이스 차단 포트 443 또는 HTTPS 프로토콜에 액세스 목록이 있는지 확인합니다.
- 파일 전송이 진행되는 동안 네트워크 디바이스에 패킷 캡처를 수행합니다.



참고: HTTPS 파일 전송 테스트를 완료한 후 명령을 사용하여 cisco-bridge.png 파일을 제거하십시오. delete flash:cisco-bridge.png

---

네트워크 장치의 HTTPS 클라이언트 소스 인터페이스

네트워크 디바이스 클라이언트 소스 인터페이스가 올바르게 구성되었는지 확인합니다.

컨피그레이션을 검증하기 show run | in http client source-interface 위해 다음 명령을 실행할 수 있습니다.

MXC.TAC.M.03-1001X-01#show run | in http client source-interface

ip http client source-interface GigabitEthernet0
MXC.TAC.M.03-1001X-01#

디바이스에 잘못된 소스 인터페이스가 있거나 소스 인터페이스가 없는 경우 HTTPS 전송 파일 테스트가 실패합니다.

예를 살펴보겠습니다.

랩 디바이스는 인벤토리 Cisco DNA Center에 IP 주소 10.88.174.43이 있습니다.

인벤토리 스크린샷:

Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability
MXC.TAC.M.03-1001X-01.etlecuit.mx	10.88.174.43	Routers	Reachable	Not Scanned	Managed

HTTPS 파일 전송 테스트 실패:

MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
%Error opening https://10.x.x.x/core/img/cisco-bridge.png (I/O error)
MXC.TAC.M.03-1001X-01#

소스 인터페이스 확인:

<#root>

MXC.TAC.M.03-1001X-01#show run | in source-interface
ip ftp source-interface GigabitEthernet0

ip http client source-interface GigabitEthernet0/0/0

```
ip tftp source-interface GigabitEthernet0
ip ssh source-interface GigabitEthernet0
logging source-interface GigabitEthernet0 vrf Mgmt-intf
```

인터페이스 확인:

MXC.TAC.M.03-1001X-01#show ip int br | ex unassigned
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 1.x.x.x YES manual up up
GigabitEthernet0 10.88.174.43 YES TFTP up up

MXC.TAC.M.03-1001X-01#

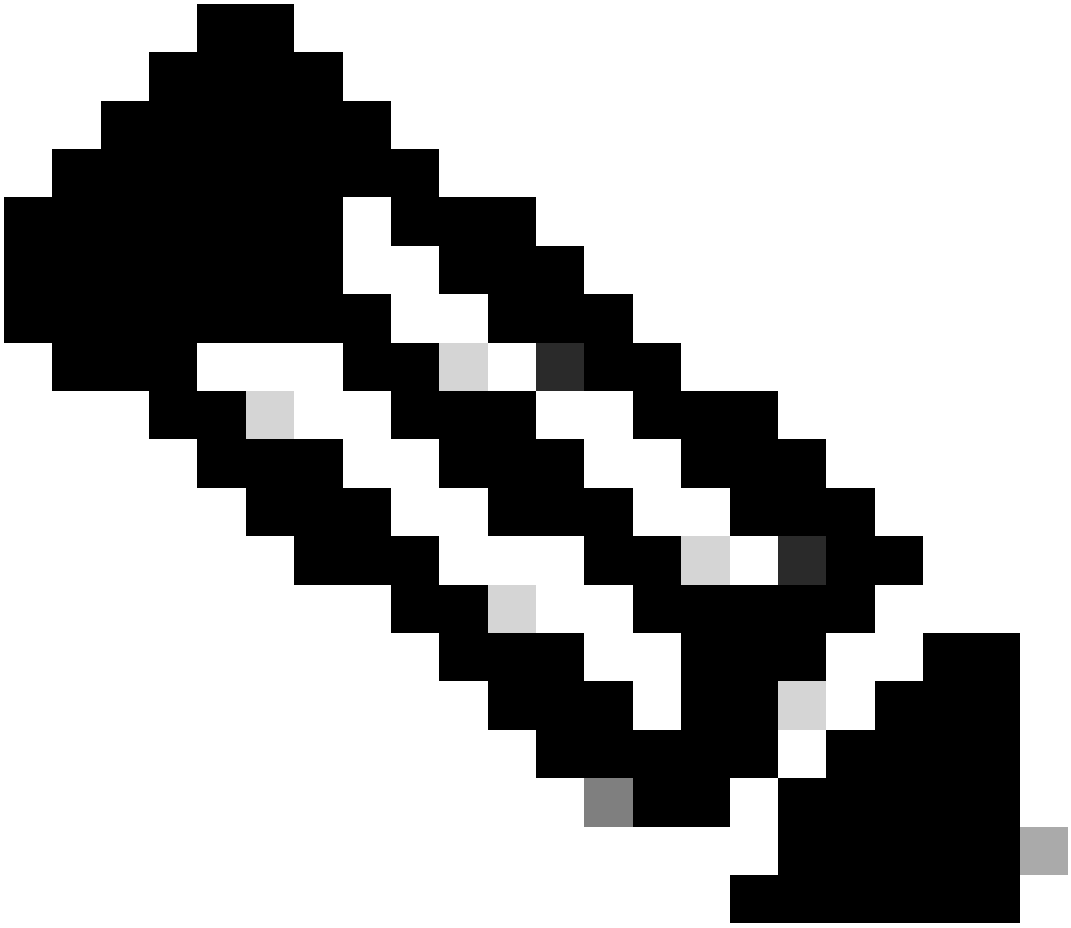
Inventory(인벤토리) 스크린샷에 따르면 Cisco DNA Center는 GigabiEthernet0/0/0 대신 GigabitEthernet0 인터페이스를 사용하는 디바이스를 발견했습니다

문제를 해결하려면 올바른 소스 인터페이스로 수정해야 합니다.

MXC.TAC.M.03-1001X-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MXC.TAC.M.03-1001X-0(config)#ip http client source-interface GigabitEthernet0
MXC.TAC.M.03-1001X-0(config)#

MXC.TAC.M.03-1001X-01#show run | in source-interface
ip ftp source-interface GigabitEthernet0
ip http client source-interface GigabitEthernet0
ip tftp source-interface GigabitEthernet0
ip ssh source-interface GigabitEthernet0
logging source-interface GigabitEthernet0 vrf Mgmt-intf
MXC.TAC.M.03-1001X-01#

MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
Loading https://10.x.x.x/core/img/cisco-bridge.png
4058 bytes copied in 0.126 secs (32206 bytes/sec)
MXC.TAC.M.03-1001X-01#



참고: HTTPS 파일 전송 테스트를 완료한 후 명령을 사용하여 cisco-bridge.png 파일을 제거하십시오. delete flash:cisco-bridge.png

---

날짜 동기화

명령을 사용하여 네트워크 장치에 올바른 날짜와 시계가 있는지 확인합니다 show clock

DNAC-CA 인증서가 LAB 디바이스에 없는 실습 시나리오를 살펴보십시오. 텔레메트리 업데이트가 푸시되었지만 다음 이유로 DNAC-CA 인증서 설치가 실패했습니다.

Jan 1 10:18:05.147: CRYPTO_PKI: trustpoint DNAC-CA authentication status = 0
%CRYPTO_PKI: Cert not yet valid or is expired -
start date: 01:42:22 UTC May 26 2023
end date: 01:42:22 UTC May 25 2025

보시다시피 인증서가 유효합니다. 그러나 오류가 발생하여 인증서가 아직 유효하지 않거나 만료되었습니다.

네트워크 디바이스 시간 확인:

MXC.TAC.M.03-1001X-01#show clock
10:24:20.125 UTC Sat Jan 1 1994
MXC.TAC.M.03-1001X-01#

날짜 및 시간에 오류가 있습니다. 이 문제를 해결하려면 ntp 서버를 구성하거나 권한 모드의 명령으로 시계를 수동clock set 으로 구성할 수 있습니다.

수동 시계 컨피그레이션 예:

MXC.TAC.M.03-1001X-01#clock set 16:20:00 25 september 2023

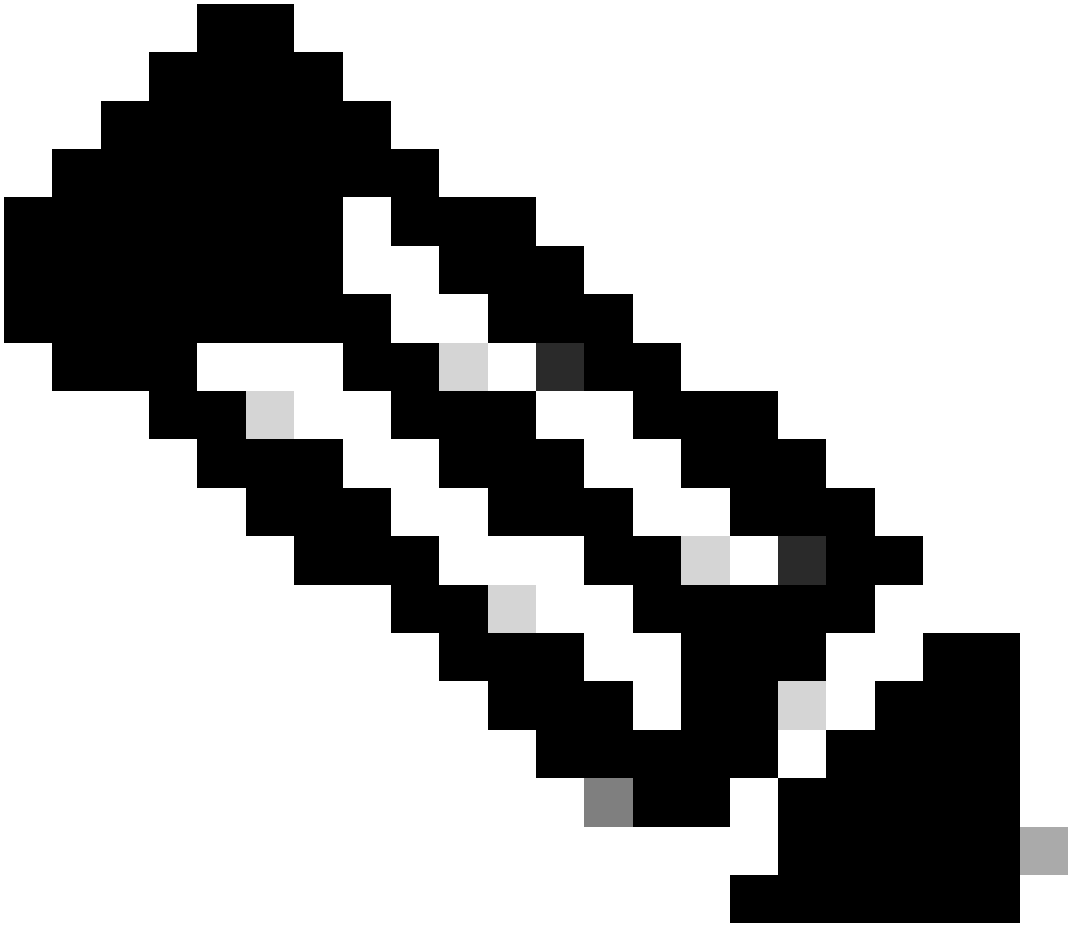
NTP 컨피그레이션 예:

MXC.TAC.M.03-1001X-0(config)#ntp server vrf Mgmt-intf 10.81.254.131

디버그

디버그를 실행하여 HTTPS 문제를 해결할 수 있습니다.

debug ip http all
debug crypto pki transactions
debug crypto pki validation
debug ssl openssl errors



참고: 네트워크 디바이스 트러블슈팅을 완료한 후 명령을 사용하여 디버그를 중지합니다 undebug all

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.